CYBER RISK MANAGEMENT:
Best Practices for the Towing Industry, Version 1.0

As part of the nation's critical infrastructure, the maritime industry has an important role to play in protecting our national security and economy. As the industry evolves to meet its needs with new technology, becoming increasingly reliant on cyber systems and connectivity of Operational Technology (OT) with Information Technology (IT), it faces new challenges. Cyber criminals are targeting the industry at unprecedented rates, and cyber disruptions – whether from an attack or from an accident – can have far-reaching consequences. The maritime industry must focus now more than ever on protecting human life, maritime assets, and the marine environment from cyber-related incidents.

AWO member companies are incredibly diverse in size and complexity, and the safeguards necessary to protect one company's cyber systems against attack and disruption may not be practicable for another's. Therefore, the Coast Guard-AWO Cyber Risk Management Quality Action Team recommends that a company take a tailored approach that incorporates cyber risks into existing risk assessment and management processes, including its Safety Management System, allowing the company to decide whether and how to mitigate its unique risks.

Basic Risk Assessment Guidelines

1. **Identify & Characterize the Computer System**
   - What function does this computer system perform? Is the function critical?
   - Who uses the computer system?
   - How is the computer system accessed? Internally or externally?

2. **Identify Risks**
   - Unauthorized access to the computer system and when? (malicious or accidental)
   - Misuse of information stored in the computer system
   - Loss of data from the computer system
   - Disruption of service of the computer system

3. **Determine Risk Impact**
   - Determine how a cyber incident for a computer system would impact company and/or vessel operations

4. **Determine Risk Probability**
   - How likely is an incident to occur?

5. **Assess Risk Rating**
   - Risk Probability X Impact of Occurrence = Risk Rating (see matrix)

6. **Determine & Implement Security Controls**
   - Administrative controls (policies and procedures)
   - Technical controls (firewalls, anti-virus software, data access permissions, etc.)
   - User training

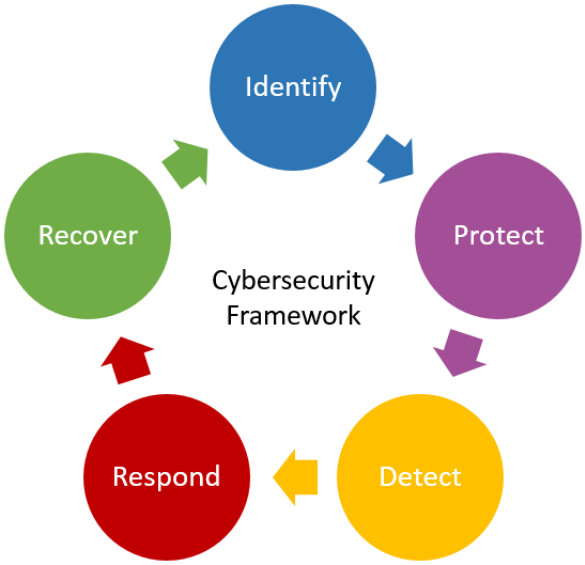
7. **Monitor**
   - Continue to monitor the security controls for effectiveness and re-evaluate risk when changes are made to the system

Risk Matrix

Risk Probability	Impact of Occurrence: Minimal	Moderate	Major	Severe
Rare	LOW (1)	LOW (1)	LOW (1)	LOW (2)
Unlikely	LOW (1)	LOW (1)	MEDIUM (2)	MEDIUM (3)
Possible	LOW (1)	MEDIUM (2)	MEDIUM (2)	HIGH (4)
Likely	LOW (2)	MEDIUM (2)	HIGH (4)	CRITICAL (6)
Almost Certain	MEDIUM (3)	HIGH (5)	CRITICAL (6)	CRITICAL (10)

Coast Guard-AWO Safety Partnership
Cyber Risk Management Quality Action Team
December 2018

The American Waterways Operators



NIST Framework

The Coast Guard has adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework as the foundation for its guidance to other segments of the maritime industry on cyber risk management. The Cyber Risk Management QAT has therefore aligned these cyber risk management best practices for the towing industry with the NIST Framework, which is used widely across industry sectors as a tool to manage cyber-related risk. The core of the NIST Framework is five concurrent and continuous functions, depicted on the left, which provide a high-level, strategic view of the lifecycle of managing cyber risk: **IDENTIFY** physical and software assets, people, data and risks; **PROTECT** assets by training users and mitigating risk; **DETECT** cyber incidents; **RESPOND** with defined response processes; and **RECOVER** assets or systems affected by cyber incidents.

Maritime Operations Specific
Shoreside Operations Specific
Maritime & Shoreside Operations

IDENTIFY

Identify and diagram all critical OT control systems.

Identify all IT assets, including computer systems and services, that the company relies on. This includes those hosted shoreside, on vessels and by 3rd party providers (licensed software [SaaS], cloud service providers, etc.). Identify those computer systems and services that are critical to the operations of the company.

Assign a designee to be responsible for cyber risk management. Analyze the risk of your OT and IT assets at least once per year. Assess the potential business impact of downtime and data loss. Prioritize those assets that are critical to company operations, such as those that impact employee safety, environmental safety and the ability of your company to conduct business.

Establish a cyber risk management policy within your company's existing Safety Management System and integrate cyber into established risk assessment and training procedures.

Identify any applicable legal and regulatory requirements regarding cyber security.

PROTECT

Ensure all system users are appropriately trained and understand their responsibilities. Integrate cyber training into established training procedures in your SMS. Training should include how to identify malicious phishing emails and the importance of protecting the integrity of physical controls and navigational systems. Users should know where to report any possible cyber incident and understand their importance in the cyber risk posture of the company and the larger national critical infrastructure of which the maritime industry is a part.

Evaluate 3rd party access to onboard vessel systems. Minimize or avoid any unattended 3rd party access, and if possible, have remote access initiated by crew. Change any default passwords from 3rd party supplied equipment.

Ensure all physical control systems (Industrial Control Systems [ICS], Supervisory Control and Data Acquisition [SCADA]) are isolated. If physical control systems must be networked, enforce network segmentation and strictly control local network and internet traffic.

Physically block access to OT access points not protected by logical means (i.e., software safeguards).

Never solely rely on AIS and GPS. Educate users on how AIS and GPS can be compromised. Coordinate and confirm AIS and GPS with port authorities and continue to train in traditional navigational skills.

Utilize Multi-Factor Authentication (MFA) for privileged and remote access to computer systems where applicable.

Use unique usernames and passwords for accounts to access computer systems.

Apply system, security and application updates on your systems regularly. Include a procedure for verifying and applying updates in your SMS.

Ensure the validity of navigation and charting software updates with the system vendor. Create a defined process in your SMS for receiving, validating and updating these systems.

Apply protective technical security controls where applicable to computer systems. Consider a "defense-in-depth" approach whereby multiple layers of security controls are in place to reduce the risk when individual controls fail.

DETECT
Join an ISAC (Information Sharing and Analysis Center) to receive information and reports about current cyber threats. Check with your local port authorities; many ports are beginning to self-start ISACs for the local maritime community.
Monitor and log network egress points and user logons for computer systems. Periodically audit computer system logs to look for unauthorized access or suspicious activity.
Encourage crew members to report any suspicious behavior or activity, as well as any unauthorized access to critical OT and IT systems and functions.
Periodically scan critical computer systems for vulnerabilities.
RESPOND
Assign a designee to be responsible for responding to cyber incidents. Develop a response plan for critical OT and IT systems, indicating who inside the company and external to the company should be communicated with, and how that communication will occur.
Incorporate lessons learned from post-incident evaluations into risk mitigation activities and updates to your response plan.
Periodically test response plans using tabletop exercises.
RECOVER
Assign a designee responsible for system and data recovery planning. Identify and document data losses and how much downtime you are willing to tolerate on your systems. Identify any legal or regulatory requirements for reporting cyber incidents.
Periodically test recovery plans using tabletop exercises.
Identify any external assistance you may require for recovery efforts. Rely on subject matter experts, industry peers and the Coast Guard as needed.
Work with your insurance policyholder to understand your coverage for cyber incidents. Many policies have exemptions and some insurers require specific policies or umbrella policies for cyber security. Ensure that both maritime and shoreside resources are covered under the policy if that is required. Many insurance companies can provide resources for both responding to and recovering from cyber incidents as part of their policies.
Incorporate lessons learned from post-recovery evaluations into your recovery plan.
Share information and lessons learned with industry peers after legal consultation.

REPORTING A CYBER INCIDENT

If you operate a Maritime Transportation Security Act (MTSA)-regulated vessel or facility, according to CG-5P Policy Letter 8-16, the Coast Guard requires you to report suspicious activity and breaches of security to:

- National Response Center (1-800-424-8802), or
- National Cybersecurity and Communications Integration Center (1-888-282-0870)

OTHER INFORMATION RESOURCES

- Coast Guard Area Maritime Security Committee (contact your Captain of the Port): Collaborate with colleagues at the port level for security and information sharing.
- Maritime Security Council: A non-profit membership organization acting as an information clearinghouse for security-related issues.
- InfraGard: An FBI public-private partnership program providing members of the critical infrastructure community with a means to share information to prevent, protect and defend against attacks.